REMARKS/ARGUMENTS

Status of the Claims

Claims 2, 3, 24-33 and 37 are cancelled.

Claims 1, 4-15, 35-36 and 38-53 are withdrawn.

Claims 16-23, 34 and 54 remain in the application.

New claims 55 and 56 have been added.

Claim Amendments

Independent claims 16 and 34 have been amended to clarify that the encrypted data content comprises encrypted video data content. That is, the pending independent claims have been amended to clarify that the plurality of encrypted sections comprises sections of a video that has been encrypted. Independent claims 16 and 34 have also been amended to explicitly recite receiving (claim 16) and transmitting (claim 34) a decryption key for an encrypted section of video data content before playback of a preceding encrypted section is complete. Dependent claims 17, 19, 20, 23 and 54 have been amended for consistency with currently amended independent claim 16.

35 U.S.C § 103 Claim Rejections

In paragraphs 11-17 of the Office Action, the Examiner rejects claims 16-18, 21 and 54 under 35 U.S.C. 103(a) as being unpatentable over Feig et al. (U.S. Patent No. 7,251,833 B2) in view of Giroux et al. (U.S. Patent Application Publication No. 2002/0078361 A1);

In paragraph 18 of the Office Action, the Examiner rejects claim 19 under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al. and further in view of Granger et al. (U.S. Patent No. 6,334,189 B1);

In paragraph 20 of the Office Action, the Examiner rejects claims 22 and 23 under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al. and further in view of Watanabe et al. (U.S. Patent No. 7,114,073 B2);

In paragraph 23 of the Office Action, the Examiner rejects claim 20 under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al. and further in view of Schull (U.S. Patent Application Publication No. 2007/0219918);

In paragraph 25 of the Office Action, the Examiner rejects claim 34 under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al.

Applicant respectfully traverses the foregoing rejections for reasons stated below.

Claims 16 and 34

Independent claims 16 and 34 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al.

With respect to independent claims 16, previously presented independent claim 16 recited destroying the decryption key for each encrypted section of data content only after at least the decryption key in respect of the next encrypted section has been received, such that at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of data content. It is important to note that this feature means that the customer processing platform will have possession of the decryption key for the current encrypted section and the decryption key for the next encrypted section. This allows the seamless playback of the encrypted data content, since the customer processing platform is able to retrieve the decryption key for the next encrypted section before playback of the preceding encrypted section is complete.

In order to clarify this operation, claim 16 is currently amended to recite:

> 16. (Currently Amended) A method of receiving and controlling playback of <u>video</u> data content at a customer processing platform, comprising:

receiving over a communications medium a plurality of encrypted sections of video data content, each of which has been encrypted using a respective encryption key; and

for each encrypted section:

receiving a respective decryption key in respect of the encrypted section before playback of a preceding encrypted section is complete;

decrypting and playing back the encrypted section using the respective decryption key; and

destroying the respective decryption key only after at least a respective decryption key in respect of a next encrypted section has been received, such that contiguous playback of the encrypted sections of video data content is provided **and** at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of video data content. (emphasis added)

Independent claim 34, which is directed to a method for controlling use of encrypted contiguous video data content downloaded to a customer data content processing device has been amended similarly to independent claim 16. Specifically, currently amended independent claim 34 recites:

34. (Currently Amended) A method for controlling use of encrypted video data content downloaded to a customer data content processing device, comprising:

receiving a request comprising customer verification information from a customer data content processing device;

comparing the customer verification information with corresponding stored customer information; and

where the customer verification information is consistent with the stored customer verification information:

billing a usage charge to an account of the customer;

transmitting to the customer data content processing device a digital key to decrypt a current portion of the encrypted video data content; and

for each subsequent portion of the encrypted video data content:

transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted video data content before playback of a preceding portion of the encrypted video data content is complete; and

causing a key for a preceding portion of the encrypted video data to be deleted from the customer data content processing device only after at least the key to decrypt the subsequent portion of the encrypted data has been received by the customer data content processing device, such that contiguous playback of the portions of encrypted video data content is provided **and** at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the encrypted video data content. (emphasis added)

Applicant respectfully submits that currently amended independent claims 16 and 34 are both novel and inventive over the cited art.

With respect to Feig et al., the Examiner acknowledges that Feig et al. fails to teach or suggest destroying any decryption key.

The Examiner has relied on Giroux et al. for allegedly teaching the destruction of decryption keys. However, as noted in Applicant's response of April 7, 2008, Giroux et al. fails to teach or even suggest the destruction of decryption keys in accordance with Applicant's claims.

Specifically, Giroux et al. requires two conditions be satisfied before a decryption key for a next encrypted section of data content is requested by a customer:

a) the decryption key for a current encrypted section is destroyed following decryption and/or display of the content of the current encrypted section; and

b) the display buffers, which the decrypted data content from the current encrypted section were loaded into, are cleared following display of the content.

Giroux et al. is intended for data contents which are not time sensitive, such as written documents. Although Giroux et al. does make reference to audio clips and video clips, it should be understood that Giroux et al. is clearly not directed to the sequential playback of sequential contiguous audio clips or video clips, as the content control processes according to Giroux et al. would prevent the seamless playback of such content. It is clear that the main thrust of Giroux et al. is to written documents, for example, see Giroux et al. [0002], which states "Electronic security systems have been proposed for managing access to electronic information and electronic documents so that only authorized users may open protected information and documents. Several software tools have been developed to work with particular document readers such as Adobe Acrobat Exchange and Adobe Acrobat Reader".

In Giroux et al., the intention of encrypting different sections of a document with different keys is to be able to control which users have access to which subsets of the document. See, for example, Giroux et al. [0014], which states " ... The document or information may also be broken down into sections using the authoring tool 102, so that certain sections within a document may have different keys and/or access policies. For example, a set of users may be allowed to view pages 1-5 of a 10-page document, while a subset of those users may be allowed to view all 10 pages of the document."

It should be clear that Giroux et al. is not in any way directed to providing seamless playback of sequential contiguous sections of encrypted video data content, rather Giroux et al. is directed to controlling access to discrete sections of data content in a non-time-sensitive manner. See, for example, Giroux et al. [0016], which states "Viewing tool 104 loads the resulting clear text into the display buffers to render the document section on a display, destroys the decrypted key, and

clears the display buffers to destroy the clear text version of the document section. The clear text will thus be visible on the display, but will not exist in electronic form in a manner that can be copied or manipulated." See also Giroux et al. [0051], which states " ... If the user 216 is authorized to access the section, the server 206 sends the decryption key and options for that section to the Application Utility 230 at the viewing user's computer 224 and the Application Utility 230 decrypts the section using the decryption key. After decrypting the section, the Application Utility 230 immediately discards/destroys the key, loads the decrypted section into the display buffers to render the decrypted section to the screen, and then clears the buffers to destroy the decrypted version of the section. When the viewing user moves to a different section, the process is repeated." It should be clear that the phrase "when the viewing user moves to a different section, the process is repeated", requires that the request for access to the "different section" be transmitted to server 206 in order to receive the decryption key for the "different section", and that according to Giroux et al., this request is only generated after the viewing user attempts to "move to a different section", i.e., only after the data for the current section has been decrypted, the current decryption key is destroyed, the decrypted data is loaded into the display buffers, rendered on the screen and subsequently cleared from the buffers. In other words, Giroux et al. does not allow the viewing user to receive the decryption key for the "different section" until after the viewing user has finished viewing the current section.

In contrast, the foregoing amendments to claims 16 and 34 clarify, for example, that the decryption key for a second encrypted section of video data content is received before playback of the first encrypted section of video data content is complete, and that the decryption key for the first encrypted section is not deleted until after at least the decryption key for the second encrypted section is received, which means that the customer processing platform is able to obtain the decryption key for the second encrypted section before playback of the first encrypted section is complete, e.g. before the decrypted content of the first encrypted section is completely displayed to a viewing user, so that the customer processing platform can begin decryption of the second encrypted section before playback of the first encrypted section is complete. This then potentially allows for the seamless playback of sequential time-sensitive video data content in a manner that could not be realized by an unimaginative person of ordinary skill in the art having regard to Feig et al. and Giroux et al.

In response to the arguments presented in Applicant's response of April 7, 2008 with regard to Giroux et al., the Examiner states, with reference to In re Venner, 262 F.2d 91, 95, 120 USPQ 193, 194 (CCPA 1958), that "it has been held that broadly providing an automatic or mechanical means to replace a manual activity which accomplishes the same result is not sufficient to distinguish over the prior art" (emphasis added). However, Applicant points out that Applicant is not arguing that the present invention provides an automatic or mechanical means that replaces a manual activity described by Giroux et al. that would accomplish the same result, rather Applicant has identified a difference between the result achieved by the process of receiving, using and destroying decryption keys according to the claimed invention and any result that may be realized by a combination of the teachings of Feig et al. and Giroux et al.

Furthermore, in response to Applicant previous arguments regarding the combination of Feig et al. and Giroux et al., the Examiner further asserts that "Giroux's customer processing platform has at most a subset of the decryption keys corresponding to the encrypted sections of data content when customer has possession of the decryption key for the current section of the encrypted information. The next key is present because when the customer moves to a different section of the encrypted content, the previous content and decryption key is deleted and the process is repeated." However, as discussed above with reference to paragraph [0051] of Giroux et al., the underlined portion of this assertion is clearly inaccurate, as the "process" that is referred to requires the customer to request the decryption key for the "different section", which according to Giroux et al. is only done after the decryption key for the previous section is destroyed and the decrypted data from the display buffers has been cleared. As such, the customer, according to Giroux et al., cannot possibly have simultaneous possession of the "next key" and the "current key".

In rejecting claims 16 and 34, the Examiner alleges that the claimed invention, as recited in claims 16 and 34 "is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable" (emphasis added). However, Applicant has demonstrated above that the claimed invention is not merely a combination of old elements, rather the claimed invention includes methods having decryption

key delivery, use and destruction steps that potentially provide a technical solution unrecognized and unresolved by either of the cited references, taken alone and in combination, thereby providing a non-obvious result.

In addition, Applicant respectfully submits that one skilled in the art would find no reason to look to Giroux et al., in so far as Giroux et al. is solely directed to controlling access to particular portions of non-time-sensitive documents and disparate non-contiguous audio/video clips, when attempting to modify the teachings of Feig et al., which are solely directed to enforcing the sequential playback of a contiguous video encrypted with a plurality of encryption keys. This is further reinforced by the fact that there is absolutely no recognition of the piracy problem associated with the time-sensitive streaming of decryption keys for playback of encrypted sections of video data content, which Applicant's claimed invention aims to address. Even if Giroux et al. does teach the destruction of decryption keys at a user's data processing device, as established above Giroux et al. fails to teach or even suggest a manner in which the decryption keys can be delivered, used and then destroyed such that time-sensitive playback of a plurality of encrypted sections of a contiguous video is possible. In fact there is absolutely no suggestion in either of the references that such a problem exists, i.e., there is no recognition in the cited references of the problems associated with providing contiguous playback of a video while also mitigating piracy of the video.

Accordingly, Applicant respectfully submits that currently amended independent claims 16 and 34 are both novel and inventive over Feig et al. and Giroux et al., as no combination of Feig et al. and Giroux et al. would render the claimed invention obvious to one of ordinary skill in the art.

Claims 17-19, 21-23 and 54

The Examiner rejects claims 17, 18, 21 and 54 under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al.

Dependent claim 19 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al. and further in view of Granger et al.

Dependent claims 22 and 23 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al. and further in view of Watanabe.

Applicant respectfully submits that Granger et al. and Watanabe fail to overcome the deficiencies of Feig et al. and Giroux et al. Accordingly, by virtue of at least their claim dependencies on independent claim 16, Applicant respectfully submits that dependent claims 17-19, 21-23 and 54 are novel and inventive over the cited references for at least the same reasons.

Claim 20

The Examiner rejects claim 20 under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al. and further in view of Schull.

Schull is directed to a method and apparatus of encouraging distribution, registration, and purchase of free copyable software and other digital information which is accessed on a User's System via a Programmer's Program. Software tools which can be incorporated into a Programmer's Program allow the User to access Advanced Features of the Programmer's Program only in the presence of a valid Password which is unique to a particular Target ID generated on an ID-Target such as the User's System. Advanced features will thus re-lock if the Password is copied to another ID-target.

In rejecting claim 20, the Examiner has pointed to Figure 1 and paragraphs [0031], [0037], [0038] and [0084] of Schull. Applicant notes that Schull was filed on May 19, 2005, which is after the filing date of the instant application, and is a continuation-in-part of U.S. Patent Application No. 09/764,293 application filed on January 19, 2001. The filing date of this earlier application appears to be the basis on which the Examiner has cited Schull. However, Applicant notes that the Figure that the Examiner has pointed to in Schull, namely Figure 1, does not appear in the earlier filed application, nor are any of paragraphs [0031], [0037], [0038], [0084] from Schull included in the earlier filed application. If the Examiner intends to maintain his rejection of claim 20 on the basis of Schull, Applicant respectfully requests that the Examiner specifically identify portions of the earlier filed application (U.S. Patent Application No. 09/764,293) that correspond to the claimed features.

Regardless, Applicant respectfully submits that Schull fails to overcome the deficiencies of Feig et al. and Giroux et al., and therefore, by virtue of at least its dependence from claim 16, claim 20 is patentable over the cited references for at least the same reasons as provided above with respect to claim 16.

New Claims 55 and 56

New claims 55 is dependent on claim 16 and recites:

> 55. The method of claim 16, further comprising, for each encrypted section:
>
> requesting the respective decryption key in respect of a next encrypted section responsive to one of a control signal and a data pattern in the decrypted data content of an encrypted section that precedes the next encrypted section. (emphasis added)

New claim 56 is dependent on claim 34 and recites:

> 56. The method of claim 34, further comprising, for each subsequent portion of the encrypted data:
>
> receiving a request from the customer data content processing device for the different key to decrypt the subsequent portion of the encrypted data, wherein the request was generated responsive to one of a control signal and a data pattern in the decrypted data content of a preceding portion of the encrypted data content during playback of the preceding portion of the encrypted data content. (emphasis added)

Basis for new claims 55 and 56 can be found, for example, at page 21, lines 17 to 22.

Applicant respectfully submits that new claims 55 and 56 recite features that further distinguish over the cited references. Specifically, new claims 55 and 56 include requests from the customer to receive each decryption key for the subsequent encrypted section, which is a feature that is completely absent from Feig et al., and while Giroux et al. does describe requesting a key to

access a subsequent encrypted section of a document, Giroux et al. certainly fails to teach or even suggest generating a request for a decryption key for the next encrypted section responsive to a control signal or a data pattern in the decrypted data content of a preceding encrypted section. The other cited reference similarly fail to teach or even suggest the features of new claims 55 and 56.

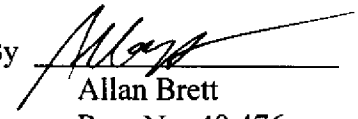
Conclusion

In view of the foregoing, Applicant respectfully submits that claims 16-23, 34, and 54-56 are both novel and inventive over the cited references, both alone and in combination, and requests that the Examiner withdraw the rejections under 35 U.S.C. 103(a).

Early favorable consideration of this application is earnestly solicited. In the event that the Examiner has concerns regarding the present response the Examiner is encouraged to contact the undersigned at the telephone number listed below.

Respectfully submitted,

VINCENT SO

By 

Allan Brett
Reg. No. 40,476
Tel.: (613) 232-2486 ext. 323

Date: February 13, 2009
RAB:JFS:gcs